**The parameter values of the current execution**

**Output**

**BGN Key Generation (K=80) -»>**

**Public Key (n, G, GT, e, g, h)**

**n(pq) = 746669815990125546932412675889809135068792550107**

**G = it.unisa.dia.gas.plaf.jpbc.field.curve.CurveField@ddfe5f49**

**GT = it.unisa.dia.gas.plaf.jpbc.field.gt.GTFiniteField@6c1a5dfd**

**e(pairing) = it.unisa.dia.gas.plaf.jpbc.pairing.a1.TypeA1Pairing@248194ae**

**g = 57629389253837384904192738648307402702024485982294,131440459530877629319843543945647747596700944293284,0**

**h = 8422102113816375511922264670321182540274850132508,13763999461410010853279216313629681971915341407732,0**

**Private Key (p)**

**p = 1075396432399422037288201**

**Vector β in CC (|β| = 10) -»> [6, 1, 4, 3, 5, 4, 8, 6, 0, 5]**

**Vector α in IoT[0] (|α| = 10) -»> [4, 9, 5, 4, 1, 0, 4, 1, 7, 3]**

**Vector α in IoT[1] (|α| = 10) -»> [8, 3, 4, 4, 1, 7, 4, 7, 6, 0]**

**Vector α in IoT[2] (|α| = 10) -»> [7, 4, 9, 0, 7, 8, 7, 1, 4, 7]**

**Vector α in IoT[3] (|α| = 10) -»> [4, 9, 5, 2, 8, 4, 6, 1, 2, 4]**

**Vector α in IoT[4] (|α| = 10) -»> [6, 7, 1, 2, 2, 7, 4, 2, 4, 5]**

**Vector α in IoT[5] (|α| = 10) -»> [4, 6, 4, 5, 6, 1, 3, 8, 3, 7]**

**Vector α in IoT[6] (|α| = 10) -»> [6, 0, 3, 0, 2, 3, 7, 4, 5, 9]**

**Vector α in IoT[7] (|α| = 10) -»> [8, 0, 9, 3, 5, 6, 8, 1, 4, 6]**

**Vector α in IoT[8] (|α| = 10) -»> [8, 7, 8, 8, 3, 3, 2, 0, 6, 1]**

**Vector α in IoT[9] (|α| = 10) -»> [3, 0, 7, 2, 8, 9, 5, 4, 0, 0]**

**Subset D\* (|D\*| = 5) -»> [4, 5, 9, 7, 1]**

**\*\*\*\*\*\*\*\*\*\* Algorithm 1 \*\*\*\*\*\*\*\*\*\***

**Vector A {E(0),E(1)}\* |A| = 10 -»> [**

**55888399770367660555852554443244888949192808965001,74632628048831694241694372564450088553815343660167,0, 175261185379752787364267063928953230699222426070274,47265905601099151771265148844740645500651260649962,0, 115896868020204068714979381996823318251674332667867,99744897315587533675931065364141470353024776739776,0, 1944793424039586341485710827713011218642399629010,44801864133394543521394200650958994011748930310770,0, 33663340092936661713134860842414417656838997031368,73708472993452755488595383226889463401702853174858,0, 131212906877464181632819450351021607671399574281905,213104468525331968249768423209698020057108068843261,0, 135545050842443762747848177583774433759620147143318,99999099789092795626127590207481272132388448435887,0, 213764131349092268537913623941373152162190093228555,81260329646018174390522050800914881752097368512911,0, 196803455418708776328894201508453038732172266029827,143009099808589073439002091697648436926449010361097,0, 73620665223443576967766496709523472781265909488995,189598599970465904110893530093189008871256076875988,0**

**]//End of Vector A**

**Vector B {E(β)} |B| = 10 -»> [**

**87829916123812062374388278322656535411267156991390,13967953632681979774135322236451362150429065319968,0, 171533077642116148141504363116938039179098326679143,895844117247749892850065179709881967678972505311,0, 171677894437252039664993621196914149765544496937764,51576907488162865536185965416433780577274516370716,0, 123042893769559017289920298777492088011354005063994,33702513313535518293685326260849371428777810541851,0, 17530488927191741093399895475341518437966967982859,69125566311443491175014003773394443611947284360189,0, 188251907363628665439798482868051265332484167619372,166117131279442046090792635288578596792372873643568,0, 212262817744821971649229898360596662548835704200679,189981599737549945181977083373075579621457763706475,0, 65381850308439119436245673829360752337011859725487,59864208479504412682838977665216812169636311789544,0, 105743953097108019107239571757031585974246252462138,151363323705555990653307015549975818918041351793176,0, 156443045841392462095245282421691311455652283328798,178864642699102103983788336619480515944921622057589,0**

**]//End of Vector B**

**\*\*\*\*\*\*\*\*\*\* Algorithm 2 \*\*\*\*\*\*\*\*\*\***

**Self Blinded Response - IoT[0] -»> 13833136673807352523975897404937508125342082230617,184219607958893514787358958296581353587978558558089,0**

**Self Blinded Response - IoT[1] -»> 155413776298175726992178984320419301800290053560887,126938294737581343241786475301004303000999145359851,0**

**Self Blinded Response - IoT[2] -»> 38137133778876105661835807184599451619391659384419,95429832558632340033881891840029325293893856885000,0**

**Self Blinded Response - IoT[3] -»> 105360438250537674953516402765662810083650557982628,73528431321607992140377303904730200663678820062901,0**

**Self Blinded Response - IoT[4] -»> 4417235102475457645094378019622195161904275370602,93737581216935854079689660516975576113715392361716,0**

**Self Blinded Response - IoT[5] -»> 188210934000571948212250824547380579923270816177648,210337614045970626356679736585605204540870126251083,0**

**Self Blinded Response - IoT[6] -»> 196101691242747578379198061221074019970680600583437,69211270749459632011914390078323733165509929565989,0**

**Self Blinded Response - IoT[7] -»> 150813831206531357922250418771927271963788391405699,130715329555726668361935559465375506314430278219490,0**

**Self Blinded Response - IoT[8] -»> 21364650382795064128028079608255691894960123319973,171292341113721159193624098792421170552698709738053,0**

**Self Blinded Response - IoT[9] -»> 39876442125842673978872580488036364582081106193307,156872843356491131040492070841242537549379455185101,0**

**Vector c {(Π B^α).h^r} |c| = 10 -»> [**

**13833136673807352523975897404937508125342082230617,184219607958893514787358958296581353587978558558089,0, 155413776298175726992178984320419301800290053560887,126938294737581343241786475301004303000999145359851,0, 38137133778876105661835807184599451619391659384419,95429832558632340033881891840029325293893856885000,0, 105360438250537674953516402765662810083650557982628,73528431321607992140377303904730200663678820062901,0, 4417235102475457645094378019622195161904275370602,93737581216935854079689660516975576113715392361716,0, 188210934000571948212250824547380579923270816177648,210337614045970626356679736585605204540870126251083,0, 196101691242747578379198061221074019970680600583437,69211270749459632011914390078323733165509929565989,0, 150813831206531357922250418771927271963788391405699,130715329555726668361935559465375506314430278219490,0, 21364650382795064128028079608255691894960123319973,171292341113721159193624098792421170552698709738053,0, 39876442125842673978872580488036364582081106193307,156872843356491131040492070841242537549379455185101,0**

**]//End of Vector c**

**\*\*\*\*\*\*\*\*\*\* Algorithm 3 \*\*\*\*\*\*\*\*\*\***

**Vector C {e(A,c)} |C|=[DStar| = 5 -»> [**

**{x=203615750547528883442758661389567688201390534454386,y=95155840890290173255326216252039085268456149664149}, {x=60250777442311639681610627792255433451923998254517,y=115182993886833678947099252826883093601373753615063}, {x=65711332806942963658579485918055660714736109245914,y=134944844986970181426408878896505638865726983311170}, {x=169807081265793946658261868902805131721785995332279,y=147014616929155847699190291058412472910840903764010}, {x=78573828349716937845712471145844123874890308401534,y=20157891147183435695237779424284613733023808808484}**

**]//End of Vector C**

**Vector β in CC (|β| = 10) -»> [6, 1, 4, 3, 5, 4, 8, 6, 0, 5]**

**Vector α in IoT[0] (|α| = 10) -»> [4, 9, 5, 4, 1, 0, 4, 1, 7, 3]**

**Vector α in IoT[1] (|α| = 10) -»> [8, 3, 4, 4, 1, 7, 4, 7, 6, 0]**

**\*\*\*\*\*\*\*\*\*\* Decryption Started in CC \*\*\*\*\*\*\*\*\*\***

**Result -»> 186 //Vector β in CC . Vector α in IoT[1] = [6, 1, 4, 3, 5, 4, 8, 6, 0, 5] . [8, 3, 4, 4, 1, 7, 4, 7, 6, 0] = (6\*8 + 1\*3 + 4\*4 + 3\*4 + 5\*1 + 4\*7 + 8\*4 + 6\*7 + 0\*6 + 5\*0) = 186**

**Result -»> 160**

**Result -»> 202**

**Result -»> 242**

**Result -»> 192**

**\*\*\*\*\*\*\*\*\*\* Decryption Ended in CC \*\*\*\*\*\*\*\*\*\***